



**UNIwersYTET
WSB MERITO
GDAŃSK**

Uniwersytet WSB Merito w Gdańsku
Wydział Informatyki i Nowych Technologii

Program studiów
Dla kierunku
„Informatyka”
Studia Drugiego Stopnia

Studia: niestacjonarne - hybrydowe

Profil: praktyczny

Rok akademicki 2026/2027

I. OGÓLNA CHARAKTERYSTYKA KIERUNKU STUDIÓW

nazwa kierunku studiów	Informatyka	
Poziom kształcenia (studia pierwszego stopnia / studia drugiego stopnia / jednolite studia magisterskie)	Studia drugiego stopnia	
Profil kształcenia	Praktyczny	
Forma studiów stacjonarne/niestacjonarne	Niestacjonarne Hybrydowe	
Czas trwania studiów (w semestrach)	4 semestry	
Łączna liczba punktów ECTS dla danej formy studiów.	120	
Łączna liczba godzin określona w programie studiów	Studia stacjonarne -	Studia niestacjonarne 3002 h
Tytuł zawodowy nadawany absolwentom	Magister	
Wymiar praktyk zawodowych.	480 h	
Język prowadzenia studiów	Polski	
Rok rozpoczęcia cyklu kształcenia	2026/2027	

II. EFEKTY UCZENIA SIĘ

Symbol efektu	Opis efektów uczenia się	Kod uniwersalnej charakterystyki
Wiedza absolwent zna i rozumie		
I2_W01	metody i modele matematyczne niezbędne do opisu i analizy zjawisk zachodzących w modelowanej rzeczywistości	P7S_WG1
I2_W02	metody, techniki i narzędzia informatyczne stosowane do rozwiązywania złożonych problemów informatycznych	P7S_WG1
I2_W03	zakres i funkcjonowanie współczesnych systemów informatycznych, teleinformatycznych, lokalnych i globalnych sieci komputerowych i nowoczesnych systemów mobilnych	P7S_WG1
I2_W04	zasady projektowania, funkcjonowania i zarządzania systemami i sieciami informatycznymi	P7S_WG1
I2_W05	zasady projektowania i analizy zaawansowanych algorytmów	P7S_WG1
I2_W06	metody stosowane do modelowania zjawisk i tworzenia oprogramowania w modelu obiektowym	P7S_WG1
I2_W07	metody wykorzystywane do zaawansowanej analizy danych i do symulacji komputerowej	P7S_WG1

I2_W08	podstawy metodologii badań naukowych i zasady tworzenia instrumentów badawczych w zakresie nauk technicznych	P7S_WG1
I2_W09	teorię oraz praktyczne aspekty dotyczące stosowanych metod, technik i narzędzi w obszarze zarządzania projektami i usługami IT oraz rozwijania form indywidualnej przedsiębiorczości w tych obszarach	P7S_WK3 P7S_WG1
I2_W10	teoretyczne i praktyczne aspekty zagadnień realizowanych w obszarach ścieżek specjalizacyjnych, obejmujące m.in. konstruowanie, zarządzanie lokalnymi i globalnymi sieciami teleinformatycznymi oraz projektowanie, programowanie i zarządzanie systemami mobilnymi	P7S_WG1
Umiejętności absolwent potrafi		
I2_U01	posługiwać się zaawansowanymi metodami, technikami i narzędziami informatycznymi do rozwiązywania złożonych problemów informatycznych oraz planować i wykonywać eksperymenty w tej dziedzinie	P7S_UW1 P7S_UW4
I2_U02	identyfikować i formułować (strukturalizować) problemy badawcze pozwalające na analizę złożonych procesów i zdarzeń w obszarach stosowania technologii IT w skali organizacji	P7S_UW1, P7S_UW2
I2_U03	krytycznie ocenić istniejące systemy informatyczne i zaproponować ich poprawienie/optymalizację	P7S_UW1
I2_U04	wykorzystać wiedzę z zakresu języków formalnych do rozwiązywania problemów z zakresu komunikacji człowiek-komputer, sztucznej inteligencji, formułowania algorytmów i projektowania systemów informatycznych	P7S_UW1
I2_U05	wykorzystać nabytą wiedzę do opisu procesów, tworzenia modeli, zapisu algorytmów oraz używać symulacji komputerowych do analiz i projektowania baz danych, tworzenia aplikacji internetowych, systemów i sieci komputerowych	P7S_UW1
I2_U06	analizować cechy systemów informatycznych lub związanych z nimi artefaktów; wyciągać wnioski i formułować rekomendacje dotyczące organizacji i zarządzania systemami informatycznymi	P7S_UW1, P7S_UW2
I2_U07	projektować i wdrażać średniozaawansowane i złożone rozwiązania techniczne i technologiczne w wybranym obszarze informatyki	P7S_UW1 P7S_UW4
I2_U08	prezentować zdobytą wiedzę i umiejętności w mowie i piśmie z wykorzystaniem m.in. narzędzi informacyjnych	P7S_UK1
I2_U09	komunikować się i prowadzić dyskusję na tematy specjalistyczne w środowisku zawodowym oraz w innych kręgach odbiorców	P7S_UK2
I2_U10	posługiwać się językiem obcym również w zakresie nauk technicznych na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego	P7S_UK3
I2_U11	kierować zespołem i pracować jako członek zespołu	P7S_UO1 P7S_UO2
I2_U12	samodzielnie zdobywać i doskonalić wiedzę oraz umiejętności zawodowe	P7S_UU
Kompetencje społeczne absolwent jest gotów do		
I2_K01	przyjmowania odpowiedzialności za powierzone mu zadania	P7S_KR
I2_K02	samodzielnego podejmowania decyzji i wykorzystywania wiedzy w rozwiązywaniu problemów poznawczych i praktycznych	P7S_KK1 P7S_KK2
I2_K03	dzielenia się wiedzą, tworzenia i rozwijania wzorów właściwego postępowania w środowisku pracy i życia	P7S_KO1

**III. ZAJĘCIA LUB GRUPY ZAJĘĆ NIEZŁĄCZNIEM OD FORMY PROWADZENIA
WRAZ Z PRZYPISANIEM DO NICH EFEKTÓW UCZENIA SIĘ I TREŚCI
PROGRAMOWYCH ZAPEWNIAJĄCYCH UZYSKANIE EFEKTÓW**

ZAJĘCIA LUB GRUPY ZAJĘĆ	ODNIESIENIE DO KIERUNKOWYCH EFEKTÓW UCZENIA SIĘ	TREŚCI PROGRAMOWE
Podstawy teleinformatyki	I2_W03, I2_U05, I2_U11, I2_K01	Podstawowe pojęcia: linie teletransmisyjne Źródła napięcia i prądu, Rezystancja i impedancja Dopasowanie źródła. Zasada przekazywania maksimum mocy Dwójnik o rezystancji R Dwójnik o indukcyjności L Dwójnik szeregowy o pojemności C, Obwód RLC, Rezonans napięć Rezonans prądów Elementy algebry czwórników. Transmisja sygnału w linii Definicja i własności logarytmu, Moc i wzmocnienie napięciowe wyrażone w decybelach, Pojęcie i definicja linii długiej Model linii długiej jako czwórnika Parametry transmisyjne kabli Impedancja i tłumność falowa Transmisja danych w sieci i fizyczne łącza Pasma cyfrowe. Prawo Shannona Algorytmy kodowania danych Krótka charakterystyka wybranych wersji standardu Ethernet Rodzaje, budowa i parametry skrętki Budowa i parametry kabla koncentrycznego Budowa i działanie światłowodów. Sieci transmisyjne Telekomunikacja Łańcuch informacyjny i telekomunikacyjny Tor teletransmisyjny Natężenie ruchu telekomunikacyjnego Transmisja analogowa a cyfrowa Komutacja Pole komutacyjne Modulacja Transmisja wąsko, szerokopasmowa Standard ISDN Sieć SMDS Asynchroniczny typ transferu danych ATM Sieć GSM Standard GPRS UMTS Sieci pagerowe. Sieciowe systemy satelitarne Telefonía komputerowa. Sieci inteligentne.
Projektowanie systemów informatycznych	I2_W03, I2_W04, I2_W08, I2_U03, I2_U05, I2_U06, I2_U10, I2_U11 I2_K01, I2_K02	Zaawansowane aspekty projektowania obiektowego. Rozbudowane diagramy UML (przypadków użycia, czynności, klas, powiązania pomiędzy diagramami) - przypomnienie. Metodologie projektowania i wdrażania systemów informatycznych. - metody zwinne (Scrum, Crystal, FDD, XP, Internet Speed Development) - metoda projektowania systemów zmiennych w czasie (DSDM – ang. Dynamic Systems Development Method). Zarządzanie jakością w zastosowaniu do projektowania systemów informatycznych. - Zapewnienie jakości oprogramowania - rodzina norm ISO 9000. - Kryterium niezawodności działania systemów. Zasada data protection by design. Zagadnienia prywatności w fazie projektowania – zasady: podejście proaktywne (zaradcze); prywatność jako ustawienie domyślne; prywatność włączona w projekt; pełnej funkcjonalności; ochrony od początku do końca cyklu życia informacji; widoczności i przejrzystości; poszanowania dla prywatności użytkowników. Rozporządzenie ogólne o ochronie danych osobowych (RODO) w aspekcie projektowaniu systemów informatycznych. Zagrożenia w systemach informatycznych - typy zagrożeń, -

		przeciwdziałanie zagrożeniom, - bezpieczeństwo transakcji, - wybrane (stosowane w praktyce) algorytmy kryptograficzne. Zaawansowane narzędzia CASE. Klasyfikacja i przykłady narzędzi. Zaawansowane, automatyczne generowanie kodu oraz dokumentacji z wykorzystaniem komercyjnych narzędzi CASE dla różnych języków programowania.
Metodologia badań naukowych	I2_W07, I2_U02, I2_U07, I2_U08, I2_K01, I2_K03	Pojęcie metody naukowej, weryfikacji, falsyfikacji, założenia i tezy - w teorii i praktyce. Krytyka, dyskurs naukowy, sceptycyzm, racjonalizm i empiryzm - wstęp do metody naukowej. Krytyka, dyskurs naukowy, sceptycyzm, racjonalizm i empiryzm - wstęp do metody naukowej. Metodologia dokumentowania pracy naukowej: badania, dyskusja wyników, artykuł naukowy, źródła, weryfikowalność wyników. Zagadnienia prawne w metodologiach naukowych - swoboda nauki, ochrona własności intelektualnej, zagadnienie plagiatu i autoplagiatu
Inteligencja obliczeniowa	I2_W01, I2_W02, I2_W06, I2_W10, I2_U02, I2_U04, I2_U11, I2_U12, I2_K01, I2_K02	Wprowadzenie do środowiska R, Wykorzystanie algorytmów genetycznych w: - problemie plecakowym - problemie labiryntu -problemie 3-SAT Wizualizacja działania algorytmu genetycznego. Logika rozmyta. Użycie logiki rozmytej do rozwiązania problemów praktycznych jak ocena ryzyka związanego z klientem w branży ubezpieczeniowej czy obliczenie składki polisy ubezpieczeniowej w zależności od parametrów np. opisujących zdrowie klienta. Obróbka danych w środowisku R. Czyszczenie, preprocessing i zmniejszanie wymiarowości danych. Klasyfikacja za pomocą drzew. Pisanie klasyfikatorów w środowisku R. Macierz błędów. Algorytmy klasyfikujące: k-Najbliższych Sąsiadów (kNN) i Naive Bayes, Wprowadzenie do sieci neuronowych. biologiczny model neuronu, klasyfikacja binarna, perceptron prosty. Uczenie nadzorowane. uczenie nienadzorowane. Problem "przeuczenia". Algorytmy grupujące. Algorytm k-średnich. Asocjacje. Obliczanie wsparcia i wiarygodności reguł asocjacyjnych. Zgłębianie tekstu. Chmury słów. Tworzenie Document-Term-Matrix do znajdowania podobieństwa dokumentów.
Języki formalne i złożoność obliczeniowa	I2_W01, I2_W02, I2_W10, I2_U4, I2_U11, I2_U12, I2_K01, I2_K02	Alfabety i języki. Wyrażenia regularne i wzorce. Deterministyczne automaty skończone (DAS). Niedeterministyczne automaty skończone (NAS). Równoważność automatów skończonych i wyrażeń regularnych. Języki i gramatyki bezkontekstowe. Postać normalna Chomsky'ego. Lemat o pompowaniu dla języków bezkontekstowych. Testowanie, czy dany łańcuch należy do danego języka bezkontekstowego: algorytm Cocke'a-YoungeraKassamiego (CYK) Automaty ze stosem (AZS). Maszyny Turinga i obliczalność. Języki obliczalne, częściowo obliczalne i nieobliczalne. Klasy złożoności obliczeniowej. Wielkie problemy złożoności obliczeniowej.
Język obcy techniczny - IT	I2_W07, I2_U07, I2_U08, I2_U09, I2_U11, I2_K03	Specyfika komunikacji technicznej - słownictwo, konstrukcja przekazu, treść, formatowanie. Manual i instrukcja użytkownika - pomiędzy językiem naturalnym a

		dokumentacją techniczną. Specyfika zagadnienia, przykłady. Artykuł naukowy w języku obcym - specyfika doboru słownictwa, struktury i budowy materiału. Artykuł popularno-naukowy w języku obcym. Mówiony i pisany język techniczny w komunikacji codziennej: mail, memo, aide-memoire, prezentacja (także: multimedialna) w języku obcym. Komunikacja praktyczna.
Wielowymiarowa analiza danych	I2_W01, I2_W02, I2_W05, I2_W06, I2_W10, I2_U01, I2_U02, I2_U04, I2_U07, I2_U11, I2_K01, I2_K02	Podstawowe zagadnienia analizy danych. Obiekty i zmienne. Klasyfikacja zmiennych. Modele ARIMA, ARMA. Metoda KMNK. Skale pomiarowe i ich charakterystyka. Analiza dyskryminacyjna. Analiza skupień. Analiza czynnikowa Wybrane elementy taksonomii. Analiza logarytmiczno-liniowa.
Seminarium dyplomowe	I2_W07, I2_U07, I2_U08, I2_U11, I2_K01	Przedstawienie wymagań dotyczących zawartości i redakcji pracy dyplomowej Sformułowanie tematów prac i określenie celów, szczegółowych wymagań i ograniczeń dla zadań technicznych zawartych w konkretnych pracach Omówienie metodologii pracy przy realizacji inżynierskiej pracy dyplomowej Zasady korzystania z literatury. Dokumentowanie źródeł, cytowania. Problemy własności intelektualnej – aspekty prawne i etyczne Metody i narzędzia prezentacji wyników, prezentacje i dyskusje dotyczące poszczególnych prac Uwrażliwienie na problematykę samodzielności pracy i ochrony praw autorskich
Zarządzanie systemami i sieciami informatycznymi	I2_W03, I2_W04, I2_U03, I2_K03	Wprowadzenie do zarządzania systemami i sieciami informatycznymi: zadania i obszary zarządzania, koncepcja metody zarządzania. Zarządzanie systemami otwartymi OSI, warstwa aplikacji systemu zarządzania (elementy usługowe ACSE, RTSE, ROSE, CMISE, SMASE, CCRSE, TPASE i FTAMASE), notacja składni abstrakcyjnej ASN.1, struktura informacji zarządzania (notacje GDMO i IDL - definiowanie zarządzanych obiektów), przesyłanie informacji zarządzania (protokół CMIP), przegląd funkcji zarządzania systemami; Sieć zarządzania telekomunikacją TMN architektura sieci TMN, metodyka specyfikowania interfejsów sieci TMN, generyczny model informacyjny sieci TMN, przegląd usług i funkcji zarządzania TMN; Zarządzanie sieciami wykorzystującymi protokoły rodziny TCP/IP: model zarządzania siecią Internet, struktura informacji zarządzania, protokoły SNMPv1, SNMPv2 i SNMPv3, zdalne monitorowanie RMON; Przegląd systemów zarządzania sieciami Bazy informacji zarządzania MIB, MIB-II, RMON MIB; Zarządzanie systemami oparte na polityce; Zarządzanie systemami oparte na intersieci Web, architektura WIMA; Zarządzanie sieciami a przetwarzanie rozproszone: środowisko DME, architektura CORBA, architektura TINA; Przegląd systemów zarządzania sieciami ISDN, SDH, ATM, LAN, MAN, WAN, GSM i SS7 oraz systemami dystrybucji i wyszukiwania informacji MHS i Directory
Zarządzanie bezpieczeństwem informacji - warsztaty	I2_W03, I2_W04, I2_U03, I2_K03	Bezpieczeństwo informacyjne i bezpieczeństwo informacji przetwarzanej w systemach teleinformatycznych Podstawowy standard definiujący System Zarządzania Bezpieczeństwem Informacji Technologiczne aspekty w bezpieczeństwie informacji Wdrażanie rozwiązań

		zarządzania bezpieczeństwem informacji warsztat Identyfikowania procesów zarządzania ryzykiem w zakresie bezpieczeństwa informacji- warsztaty
Internet rzeczy	I2_W03, I2_W04, I2_U01, I2_U02, I2_U06, I2_U11	Wprowadzenie – definicja Internetu rzeczy, przykłady aplikacji, architektura systemu: warstwy, protokoły, pakiety, usługi, wydajność systemów, P2P, sieci czujników. Sprzętowa realizacja urządzeń IoT – systemy wbudowane i ich architektura, akwizycja danych, pomiary i sterowanie, oprogramowanie, komunikacja, RTOS. Akwizycja danych dla IoT: RFID, karty zbliżeniowe, czujniki, kody QR i kreskowe, sieci czujników. Warstwa dostępu do sieci dla IoT (technologie przewodowe i bezprzewodowe), warstwa sieciowa (adresy IP, DNS, NAT, routery), transportowa. (TCP/UDP) Przetwarzanie danych – chmura i mgła obliczeniowa Zastosowania – inteligentny budynek, automatyzacja produkcji i magazynowania, sieci energetyczne, monitorowanie środowiska, opieka medyczna, systemy transportowe
Przedmioty do wyboru	I2_W02, I2_W04, I2_W07, I2_U01, I2_U02, I2_U03, I2_U05, I2_K02	<i>Architektura korporacyjna</i> (poznanie różnych ram architektury korporacyjnej ze szczególnym uwzględnieniem TOGAF, opanowanie wiedzy z zakresu identyfikowania elementów i tworzenia architektury korporacyjnej, umiejętność analizy systemu informacyjnego przedsiębiorstwa w kontekście jego architektury korporacyjnej), <i>Bezpieczeństwo danych</i> (zapoznania studenta m.in. z następującymi zagadnieniami: Przeprowadzenie i analiza ataku na system / aplikację, Przykładowe ataki na użytkowników systemów, Konstrukcja i testowanie systemów wysokodostępnych, Analiza ryzyka systemów informatycznych).
Zaawansowane techniki obiektowe	I2_W01, I2_W02, I2_W05, I2_U01, I2_U04, I2_U06, I2_U07, I2_U11, I2_K1	Konstrukcja systemów obiektowych Zasady SOLID Rodzaje wzorców projektowych Rola wzorców projektowych Dług projektowy, refaktoryzacja i podejścia TDD/BDD Elementy DDD, AoP
Wprowadzenie do praktyk zawodowych	INF_I_inż_W04 INF_I_inż_U03 INF_I_inż_K01	Zapoznanie studentów z regulaminem i zasadami realizacji praktyk zawodowych
Praktyka zawodowa	I2_W03, I2_W08, I2_W09, I2_U05, I2_U07, I2_U08, I2_U09, I2_U11, I2_K01, I2_K02, I2_K03	Podstawy prawne i przedmiot działalności instytucji. Status prawny, struktura własnościowa, przedmiot i zakres działalności instytucji. Misja i strategia instytucji. Organizacja podmiotu gospodarczego i zakresu jego działalności. Struktura organizacyjna, uprawnienia decyzyjne i zakres odpowiedzialności poszczególnych komórek. Dokumentacja organizacyjna instytucji. Statut, regulaminy, instrukcje i zasady obiegu dokumentów. Zakres obowiązków na stanowisku pracy Zapoznanie się z metodami pracy na stanowisku Współuczestnictwo w realizacji zadań organizacyjnych
General electives	I2_W02, I2_W03, I2_W04, I2_W05, I2_W08, I2_W09, I2_U02,	Przedmioty realizowane są w języku angielskim: Projektowanie i rozwój usług cyfrowych. Zorientowane na użytkownika podejścia do projektowania, ewaluacji i testowania. Zarządzanie projektami dla usług cyfrowych. Współpraca z klientem i przyszłymi użytkownikami.

	I2_U03, I2_U04, I2_U05, I2_U07, I2_U08, I2_U10,	Zarządzanie cyklem życia usług cyfrowych i aplikacji mobilnych. Eksploatacja, rozwój i doskonalenie.
Zarządzanie projektem - gra biznesowa	I2_W02, I2_W04, I2_W08, I2_W09, I2_U01, I2_U04, I2_U08, I2_U10, I2_U11, I2_K01, I2_K02	Główne pojęcia z zakresu zarządzania projektami (parametry projektu; trójkąt zakresu projektu; identyfikacja działań projektowych; plan wykonalności projektu, definiowanie zakresu i struktury podziału pracy -WBS, wykonalność biznesowa projektu). Identyfikacja uczestników-interesariuszy projektu i opracowanie strategii współpracy z nimi. Identyfikacja ryzyk i zarządzanie ryzykiem projektu. Planowanie cyklu projektowo-realizacyjnego; opracowanie harmonogramów prac - wykres Gantta, metoda ścieżki krytycznej. Szacowanie kosztorysu projektu; budżetowanie. Zarządzanie zespołem projektu, zarządzanie czasem, kosztami i zasobami projektu, zarządzanie jakością i zmianą, wskaźniki skuteczności zarządzania projektem (BAC, PV, AV, PP, EV, CPI, EAC) Informatyczne narzędzia wspierające zarządzanie projektami i zespołami projektowymi.
Programowanie z elementami algorytmiki	I2_W03, I2_U05, I2_U11, I2_K01	Zmienne i typy danych: deklarować zmienne i pracować z różnymi typami danych, takimi jak liczby całkowite, liczby zmiennoprzecinkowe, ciągi znaków (np. tekst) itp. Struktury kontrolne: instrukcje warunkowe (if-else) oraz pętle (for, while). Deklaracja i wywoływanie funkcji: funkcje, zorganizować kod i umożliwić jego wielokrotne użycie. Parametry i zwracane wartości: jak przekazywać parametry do funkcji i jak funkcje mogą zwracać wartości. Tablice i listy: korzystać z tablic (array) lub list, które umożliwiają przechowywanie wielu elementów w jednej zmiennej. Pozniej struktury danych, które umożliwiają przechowywanie danych w formie par klucz-wartość. Klasy i obiekty: jak tworzyć klasy i obiekty. Testowanie jednostkowe: testy jednostkowe, aby sprawdzić, czy poszczególne części kodu działają zgodnie z oczekiwaniami. Debugowanie: śledzenie błędów i debugowanie kodu.
Projektowanie UX i interfejsów użytkownika	I2_W03, I2_W04, I2_W08, I2_U03, I2_U05, I2_U06, I2_U10, I2_U11 I2_K01, I2_K02	Wprowadzenie do UX Design: Podstawowe koncepcje związane z UX. Proces projektowania UX: Etapy tworzenia produktu, od badania użytkowników po testowanie prototypów. Persona i user journey: Tworzenie person i mapowania ścieżek użytkowników. Zasady designu UI: Kolor, kontrast, typografia, układ i inne fundamentalne aspekty designu. Zasady dostępności: Projektowanie interfejsów z myślą o różnych grupach użytkowników, w tym osobach z niepełnosprawnościami. Używanie narzędzi do projektowania, takich jak Adobe XD, Sketch, Figma czy InVision. Prototypowanie interakcji: Tworzenie interaktywnych prototypów w celu testowania funkcji i przeprowadzania użytkowników przez interfejs. Projektowanie responsywne: Tworzenie interfejsów, które dostosowują się do różnych rozmiarów ekranów (smartfony, tablety, komputery). Mobile-first design: Projektowanie z myślą o użytkownikach korzystających głównie z urządzeń mobilnych. Zastosowanie animacji w celu poprawy doświadczenia użytkownika. Interakcje gestów: Projektowanie obsługi gestów dotykowych, takich jak przeciąganie, przekładanie czy zoomowanie. Podstawy

		HTML i CSS: Umiejętność komunikacji z programistami i zrozumienie podstaw kodowania.
Bezpieczeństwo systemów informatycznych	I2_W07, I2_U02, I2_U07, I2_U08, I2_K01, I2_K03	Zarządzanie Tożsamością i Dostępem (IAM): moduły do zarządzania tożsamościami użytkowników, w tym funkcje uwierzytelniania dwuetapowego, zarządzanie sesją i zarządzanie dostępem. Kryptografia: funkcje szyfrowania i deszyfrowania danych, stosując różne algorytmy kryptograficzne. Zapewnianie bezpiecznego przechowywania haseł i kluczy. Monitorowanie i Logowanie: Zabezpieczenia Warstwy Aplikacji: Zabezpieczenia przed atakami typu SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) i inne ataki warstwy aplikacji. Zabezpieczenia Warstwy Sieci: funkcje filtracji pakietów, firewall'e oraz zastosuj protokoły bezpieczne, takie jak SSL/TLS. Skrypty monitorujące ruch sieciowy. Ochrona przed Malware: skrypty i programy do skanowania plików i systemu w poszukiwaniu potencjalnych zagrożeń. Implementuj mechanizmy antywirusowe. Zarządzanie Zdarzeniami Bezpieczeństwa (SIEM): funkcje integrujące się z narzędziami SIEM, które pomagają w analizie i reakcji na zdarzenia bezpieczeństwa. Bezpieczeństwo Systemu Operacyjnego: procedury i skrypty zabezpieczające system operacyjny, m.in. poprzez ograniczanie uprawnień użytkowników, konfigurację zasad bezpieczeństwa oraz regularne aktualizacje. Zarządzanie Aktualizacjami: Mechanizmy do zarządzania aktualizacjami oprogramowania i systemów, aby zapewnić, że wszystkie luki w zabezpieczeniach są zamknięte. Zarządzanie Ryzykiem: Wprowadzanie funkcji oceny ryzyka i monitorowanie systemu pod kątem potencjalnych zagrożeń. Skrypty do szybkiego reagowania na nowe zagrożenia.
Techniki zapewniania jakości oprogramowania	I2_W01, I2_W02, I2_W06, I2_W10, I2_U02, I2_U04, I2_U11, I2_U12, I2_K01, I2_K02	Definicja testowania oprogramowania i jego rola w procesie tworzenia. Rodzaje testów: testy jednostkowe, integracyjne, systemowe, akceptacyjne. Testowanie manualne i automatyczne. Rola testów jednostkowych w programowaniu. Frameworki do testów jednostkowych (np. JUnit, NUnit, pytest). Test Driven Development (TDD) - pisanie testów przed kodem. Tworzenie testów funkcjonalnych w oparciu o wymagania. Używanie narzędzi do automatyzacji testów funkcjonalnych (np. Selenium, Appium). Definicja testów wydajności i ich znaczenie. Proces zarządzania testowaniem. Rola testowania bezpieczeństwa w cyklu życia oprogramowania. Metody testowania, takie jak testy równoważności, testy przypadków brzegowych, testy regresji. Zrozumienie CI/CD i jego roli w zapewnianiu jakości. Kontrola wersji oprogramowania. Zarządzanie konfiguracją testowanych aplikacji. Code review jako narzędzie zapewnienia jakości kodu. Testowanie interfejsów użytkownika pod kątem użyteczności.
Tworzenie aplikacji internetowych i bazodanowych	I2_W01, I2_W02, I2_W10, I2_U4, I2_U11, I2_U12, I2_K01, I2_K02	HTML5 i znaczniki semantyczne. CSS3 i style responsywne. Podstawy JavaScript i manipulacja DOM. Użycie frameworków frontendowych, takich jak React, Angular lub Vue.js. Komponenty, routing, zarządzanie stanem. Zasady projektowania interfejsu użytkownika. Narzędzia do projektowania (np. Sketch, Figma). Wybór języka programowania serwera (np. Node.js, Python, Ruby) Przesyłanie danych między frontendem a backendem

		(RESTful API, GraphQL). Asynchroniczne zapytania AJAX. SQL i modelowanie danych. Mapowanie obiektowo-relacyjne. Modelowanie danych w bazach NoSQL. Używanie protokołów bezpiecznej komunikacji (HTTPS). Optymalizacja zasobów frontendowych. Monitoring wydajności aplikacji. Korzystanie z platform chmurowych (np. AWS, Azure, Google Cloud). Użycie systemów kontroli wersji (np. Git).
Programowanie i projektowanie aplikacji obiektowych	I2_W07, I2_U07, I2_U08, I2_U09, I2_U11, I2_K03	Wprowadzenie do koncepcji obiektów, klas, dziedziczenia, enkapsulacji i polimorfizmu. Definicja klas i obiektów w językach programowania obiektowego (np. Java, C++, Python). Zależności: asocjacje, agregacje, kompozycje. Rozróżnianie pomiędzy relacjami "jest członkiem" a "jest częścią". Rysowanie i interpretacja diagramów UML (Unified Modeling Language). Diagramy klas, diagramy sekwencji, diagramy stanów. Klasy bazowe, klasy pochodne, nadpisywanie metod. Ukrywanie szczegółów implementacyjnych wewnątrz klasy. Prywatne, chronione i publiczne modyfikatory dostępu. Wykorzystanie narzędzi do testów jednostkowych. Zapisywanie i odczytywanie obiektów do/z strumienia. Mechanizmy serializacji w językach programowania. Organizacja projektu opartego na zasadach OOP. Tworzenie warstw abstrakcji i modułów. Rozwój pełnej aplikacji z wykorzystaniem programowania obiektowego. Analiza i projektowanie rozwiązań obiektowych dla konkretnych przypadków.
Projektowanie aplikacji biznesowych - projekt zespołowy	I2_W01, I2_W02, I2_W05, I2_W06, I2_W10, I2_U01, I2_U02, I2_U04, I2_U07, I2_U11, I2_K01, I2_K02	Analiza Wymagań Biznesowych: Techniki zbierania i dokumentowania wymagań. Tworzenie i analiza dokumentów wymagań biznesowych. Modelowanie danych na potrzeby aplikacji biznesowej. Wybór i implementacja odpowiedniego systemu zarządzania bazą danych. Wybór architektury (monolityczna, mikroserwisy, itp.). Projektowanie warstw aplikacji (warstwa prezentacji, warstwa biznesowa, Użycie wzorców integracyjnych (np. ESB, Message Queues). Mechanizmy zarządzania sesją użytkownika. Przechowywanie stanu aplikacji i przesyłanie go między zadaniami. Obsługa transakcji w aplikacjach biznesowych. Implementacja mechanizmów odwracalności transakcji. Projektowanie i implementacja interfejsów API. Używanie standardów (REST, GraphQL) w projektowaniu API. Skalowalność aplikacji i systemu. Strategie wdrażania (kontenery, chmura, serwery). Zarządzanie konfiguracją aplikacji w różnych środowiskach. Mechanizmy automatycznego dostarczania konfiguracji.
Bezpieczeństwo systemów i sieci komputerowych	I2_W07, I2_U07, I2_U08, I2_U11, I2_K01	Definicja podstawowych terminów i pojęć związanych z bezpieczeństwem komputerowym. Zagrożenia i ataki w cyberprzestrzeni. Systemy uwierzytelniania i autoryzacji. Kontrola dostępu do zasobów. Analiza różnych rodzajów ataków (np. phishing, malware, ataki typu Man-in-the-Middle). Działanie firewall'i i ich rola w zabezpieczaniu sieci. Filtracja pakietów w sieciach komputerowych. Zabezpieczanie systemu operacyjnego przed atakami. Analiza logów i reagowanie na incydenty. Zabezpieczanie sieci Wi-Fi. Analiza i zabezpieczanie przed atakami na sieci bezprzewodowe. Metodologia penetration testing. Narzędzia i techniki stosowane w testach

		przenikania. Bezpieczeństwo aplikacji na platformy mobilne. Bezpieczeństwo danych przechowywanych w chmurze.
Bezpieczeństwo teleinformatyczne	I2_W03, I2_U05, I2_U11, I2_K01	Bezpieczeństwo komunikacji - Analiza wybranych protokołów komunikacyjnych pod kątem bezpieczeństwa transmisji. Wykrywanie ruchu w sieci - Wykrywanie hostów w sieci komputerowej, Klasyfikacja usług sieciowych z nieznanego źródła Zabezpieczanie sieci korporacyjnej - Opis sposobu wdrażania Microsoft ISA Server w różnych konfiguracjach strefy zdemilitaryzowanej; Opis funkcjonalności oraz wdrażania zapory ogniowej dostarczanej z Microsoft ISA Server; Implementacja bezpiecznego dostępu do wewnętrznych serwerów przy wykorzystaniu Microsoft ISA Server; Konfiguracja bezpiecznego dostępu do serwera Exchange przy użyciu Microsoft ISA Server; Zagadnienia tworzenia ochrony przed szkodliwym oprogramowaniem dla komputerów klienckich, serwerów i infrastruktury sieciowej Prawne aspekty bezpieczeństwa systemów informatycznych - Status prawny działania w systemach informatycznych na terytorium RP; Międzynarodowe standardy bezpieczeństwa systemów informatycznych
Bezpieczeństwo usług opartych o chmurę	I2_W03, I2_W04, I2_W08, I2_U03, I2_U05, I2_U06, I2_U10, I2_U11 I2_K01, I2_K02	Mechanizmy uwierzytelniania, takie jak jednorazowe hasła (OTP) autoryzacja dwuetapowa. biblioteki i narzędzia umożliwiające zarządzanie tożsamościami odpowiednie biblioteki do szyfrowania danych w transmisji i przechowywaniu. szyfrowanie symetryczne, jak i asymetryczne. Funkcje monitorowania, które śledzą działania użytkowników, zmiany w konfiguracji oraz inne zdarzenia związane z bezpieczeństwem. mechanizmy audytu, aby rejestrować kluczowe operacje. skrypty lub funkcje odpowiedzialne za obsługę zdarzeń bezpieczeństwa. procesy reakcji na podejrzaną działania lub ataki. procesy zarządzania konfiguracją, tak aby nie było zbędnych otwartych punktów dostępu, nieaktualizowanych komponentów czy niezabezpieczonych konfiguracji.
Cyberprzestępczość	I2_W07, I2_U02, I2_U07, I2_U08, I2_K01, I2_K03	Definicja i zakres cyberprzestępczości. Analiza różnych rodzajów ataków, takich jak phishing, ransomware, ataki DDoS. Zrozumienie podstawowych technik używanych przez hakerów. Analiza działań i cech charakterystycznych dla różnych rodzajów malware. Zrozumienie funkcjonowania Dark Web. Techniki śledcze w cyberprzestrzeni. Wprowadzenie do cyberśledztwa. Prawne aspekty zwalczania cyberprzestępczości. Opracowywanie planów reagowania na cyberataki. Bezpieczeństwo systemów sterowania przemysłowego (ICS/SCADA). Zabezpieczanie infrastruktury krytycznej.
Zintegrowane systemy zarządzania bezpieczeństwem	I2_W01, I2_W02, I2_W06, I2_W10, I2_U02, I2_U04, I2_U11, I2_U12, I2_K01, I2_K02	Definicja i zakres cyberprzestępczości. Analiza różnych rodzajów ataków, takich jak phishing, ransomware, ataki DDoS. Zrozumienie podstawowych technik używanych przez hakerów. Analiza działań i cech charakterystycznych dla różnych rodzajów malware. Zrozumienie funkcjonowania Dark Web. Techniki śledcze w cyberprzestrzeni. Wprowadzenie do cyberśledztwa. Prawne aspekty zwalczania cyberprzestępczości. Opracowywanie planów reagowania na cyberataki. Bezpieczeństwo systemów sterowania przemysłowego (ICS/SCADA). Zabezpieczanie infrastruktury krytycznej. Definicja ISMS i jego rola w

		organizacji. Korzyści z wdrożenia zintegrowanego systemu zarządzania bezpieczeństwem. Przegląd głównych norm i standardów związanych z bezpieczeństwem informacji Proces certyfikacji i zgodności z normami. Tworzenie, wdrożenie i utrzymanie polityki bezpieczeństwa informacji. Proces reagowania na incydenty bezpieczeństwa. Tworzenie i wdrażanie planów zarządzania incydentami. Bezpieczne przechowywanie i przetwarzanie danych. Ochrona poufności, integralności i dostępności danych Ocena i zarządzanie ryzykiem związanym z dostawcami. Przegląd nowoczesnych technologii zabezpieczeń (firewall, antywirus, IDS/IPS). Integracja technologii w ramach ISMS. Tworzenie strategii zintegrowanego zarządzania bezpieczeństwem. Rola zarządzania bezpieczeństwem w ogólnej strategii organizacji.
Współczesne protokoły kryptograficzne	I2_W07, I2_U07, I2_U08, I2_U09, I2_U11, I2_K03	Podzielność i reprezentacja liczb całkowitych, systemy liczbowe. Rozszerzony algorytm Euklidesa. Kongruencje i elementy odwrotne w pierścieniu Z/mZ , efektywne algorytmy obliczenia potęgi w pierścieniu Z/mZ . Układy kongruencji liniowych: metody rozwiązania. Systemy kryptograficzne symetryczne i asymetryczne Ważne klasy szyfrów: szyfry podstawieniowe, przestawieniowe, afiniczne, Vigenera, Hilla i ich kryptoanaliza Szyfry blokowe Funkcje skrótu Szyfr RSA
Front-end aplikacji webowych	I2_W01, I2_W02, I2_W05, I2_W06, I2_W10, I2_U01, I2_U02, I2_U04, I2_U07, I2_U11, I2_K01, I2_K02	Definicja strony internetowej, strona wizytówka vs portal vs SPA narzędzia wspomagające projektowanie stron internetowych., szkic, wireframe, mockup, prototyp - omówienie różnic narzędzia do wspomagania procesów w zespole projektowym "responsive web design w praktyce, podejście mobile first, paradygmat atomic design, zbieranie wymagań klienta, konfrontowanie projektu z wymaganiami klienta
Tworzenie backendu do aplikacji webowych	I2_W07, I2_U07, I2_U08, I2_U11, I2_K01	Modele dostępu do baz danych (model scentralizowany, klient-serwer, rozproszony-architektura trójwarstwowa). Mechanizm dostępu do danych (odbieranie i wysyłanie danych, wewnętrzna reprezentacja danych, prezentacja danych w GUI, logika biznesowa do przetwarzania danych. Kompozycja aplikacji klient serwer. Nawiązywanie połączenia z wybranymi serwerami SQL Nawiązywanie połączenia z wybranymi serwerami NoSQL
Programowanie aplikacji webowych z wykorzystaniem platformy .NET, vlab	I2_W03, I2_U05, I2_U11, I2_K01	"NET Framework, LINQ, Entity Framework, Windows Presentation Foundation" Tworzenie aplikacji webowych z wykorzystaniem ASP.NET Fetch API / Ajax (XHR), ES6+, Modularność Javascript, TypeScript Testy jednostkowe, integracyjne i funkcjonalne aplikacji webowych Mocha, Chai, Ava, Jasmine, Jest, Cypress, Enzyme, React-testing-library
Programowanie aplikacji webowych w Java	I2_W03, I2_W04, I2_W08, I2_U03, I2_U05, I2_U06, I2_U10, I2_U11, I2_K01, I2_K02	Polecenia warunkowe, Pętle, Metody, ArrayList, Programowanie obiektowe, Tablice, Sortowanie, Wyszukiwanie, HashMap, Interfejsy, Wyjątki, I/O, Dziedziczenie, Graphical user interface (GUI), Wyrażenia regularne, Iteratory, Enum
RIA, Case study: Angular	I2_W07, I2_U02, I2_U07, I2_U08, I2_K01, I2_K03	Koncepcja aplikacji RIA, konfiguracja środowiska developerskiego. Angular. Usługi i dostawcy usług. Routing i

		animacja w Angularze Bindowanie danych Aplikacja mobilne PWA z Angular
Technologie tworzenia stron WWW	I2_W01, I2_W02, I2_W06, I2_W10, I2_U02, , I2_U04, I2_U11, I2_U12, I2_K01, I2_K02	Definicja strony internetowej, strona wizytówka vs portal vs SPA, narzędzia wspomagające projektowanie stron internetowych, szkic, wireframe, mockup, prototyp - omówienie różnic, narzędzia do wstępnego szkicowania, narzędzia do budowania wireframe-ów, narzędzia do budowania mocków narzędzia do budowania prototypów, narzędzia do wspomagania procesów w zespole projektowym, responsive web design w praktyce, podejście mobile first , paradygmat atomic design, narzędzia developera dostępne w przeglądarce, zbieranie wymagań klienta, konfrontowanie projektu z wymaganiami klienta
Tworzenie aplikacji PWA	I2_W01, I2_W02, I2_W10, I2_U4, I2_U11, I2_U12, I2_K01, I2_K02	PWA - koncepcja internetowych aplikacji mobilnych PWA - konfiguracja aplikacji Manifest aplikacji PW ServiceWorker w aplikacjach PWAMobilne bazy danych - offline

IV. PRZYPORZĄDKOWANIE KIERUNKU STUDIÓW DO DYSYCYPLIN NAUKOWYCH

L.p.	Dyscypliny naukowe	% PUNKTÓW ECTS
1.	Informatyka (dyscyplina wiodąca)	81

V. PODSTAWOWE WSKAŹNIKI ECTS OKREŚLONE DLA PROGRAMU STUDIÓW

Nazwa wskaźnika	Liczba punktów ECTS/Liczba godzin
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	STUDIA NIESTACJONARNE N/D
Łączna liczba punktów ECTS przyporządkowana zajęciom kształtującym umiejętności praktyczne	105,5
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych lub nauk społecznych – w przypadku kierunków studiów przyporządkowanych do dyscyplin w ramach dziedzin innych niż odpowiednio nauki humanistyczne lub nauki społeczne	6
Łączna liczba punktów ECTS przyporządkowana zajęciom do wyboru	76,6
Łączna liczba punktów ECTS przyporządkowana praktykom zawodowym	20

VI. WYMIAR, ZASADY I FORMY ODBYWANIA PRAKTYK ZAWODOWYCH

Wymiar: 480 godzin praktyk zawodowych.

Student wyznaczoną liczbę godzin (w sumie) musi odbyć do końca trybu kształcenia.

Student ma możliwość zorganizowania praktyki indywidualnie bądź z pomocą Biura Obsługi Studenta.

Student udający się na odbycie praktyk zawodowych, powinien wypełnić oświadczenie wstępne, na podstawie którego tworzona jest umowa oraz skierowanie (dla pracodawcy) jak również zaświadczenie o odbytej praktyce, program praktyk, karta czasu pracy praktykanta oraz efekty kształcenia. Po zakończonych praktykach student dostarcza całą dokumentację na uczelnię, gdzie jest ona opiniowana przez opiekuna praktyk.

Praktyki zawodowe mogą odbywać się w formie stacjonarnej lub hybrydowej.

VII. SPOSOBY WERYFIKACJI I OCENY EFEKTÓW UCZENIA SIĘ OSIĄGANÝCH PRZEZ STUDENTA W TRAKCIE CAŁEGO CYKLU KSZTAŁCENIA DLA DANEGO KIERUNKU STUDIÓW

Metoda weryfikacji/Obszary	Wiedza	Umiejętności	Kompetencje społeczne
Test, kolokwium	X	X	
Egzamin pisemny	X	X	
Egzamin ustny	X	X	
Projekt	X	X	X
Referat	X	X	
Prezentacja	X	X	X
Esej	X	X	X
Wypowiedź ustna indywidualna	X	X	
Uczestnictwo w dyskusji		X	X
Studium przypadku (case study)	X	X	
Raport, sprawozdanie z zadania terenowego	X	X	
Zadania praktyczne		X	X
Samodzielne rozwiązywanie zadań		X	
Aktywny udział w zajęciach		X	X
Obserwacja studentów przez nauczyciela akademickiego			X
Praca magisterska	X	X	
Egzamin dyplomowy	X	X	

Formy i metody prowadzenia zajęć oraz kryteria oceny i jej składowe dla poszczególnych zajęć określa karta przedmiotu.